暗号規制に反対します―日本政府は「エンドツーエンド暗号化及び公共の安全に関するインターナショナル・ステートメント」から撤退を!!

日本政府は、2020年10月11日に発出された「エンドツーエンド暗号化及び公共の安全に関するインターナショナル・ステートメント」(以下「ステートメント」と呼ぶ)に、英国、米国、オーストラリア、ニュージーランド、カナダ、インドとともに署名しました。私たちは以下の理由から、このステートメントに反対します。

(1) 憲法21条で定められた「通信の秘密」条項に明確に違反します。

(2) ステートメントは、暗号化の意義を強調する一方で、例外的に法執行機関などが読取・利用できるように暗号化を弱体化させる技術の導入をIT業界に要求するという矛盾した内容になっています。私たちは、暗号化に例外を設けることに反対します。

(3) ステートメントは、暗号化への規制は「社会の非常に脆弱なメンバー」の保護に欠かせないと主張していますが、人権活動家、ジャーナリストなどによる広範な支援や当事者のプライバシーもまた暗号化によって保護され、暗号規制は「脆弱な人びと」をより脆弱にしてしまうという側面を軽視しています。

(4)ステートメントは、その表向きの理由とは裏腹に、法執行機関が私たちの通信の秘密に対して特権的な権限を行使できるような通信インフラを構築し、監視国家化を促すものです。「脆弱な人びと」含む全ての人びとのコミュニケーションの権利と基本的人権の侵害を招くことになります。

以上の理由から、私たちは、「エンドツーエンド暗号化及び公共の安全に関するインターナショナル・ステートメント」に反対し、日本政府がこのステーメントから撤退することを求めます。

2021年3月
JCA-NET理事会

(注)エンド・ツー・エンド暗号化とは、送信者と受信者の間の通信の秘密を保持する暗号化の仕組みで「サービスを提供する企業を含め、第三者が通信にアクセスすることはできない。暗号化はまた、コンピュータ、携帯電話、その他のデジタル機器に保存されている情報を保護し、機器が紛失したり盗まれたりしても、機器の情報を確実に保護するのに役立つ」。(グローバル暗号化連合の声明より)

ステートメントの背景説明

日本国憲法21条について。
憲法21条の条文は以下のとおり。
「集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。
2 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。」

ステートメンでは、暗号化によって保護されている通信に対して、捜査機関が暗号を解読できるようにテクノロジー企業に求めている。これは、憲法が明記している通信の秘密の権利を政府が率先して侵害する政策をとることを意味している。日本政府は、外交であっても憲法に反する行為を行なうことはできない。また、実際にエンド・ツー・エンド暗号化に対して捜査機関によるアクセス可能な仕組み(一般に「バックドア」と呼ばれている)を設けることを「業界に強く要求する」ということは、公権力による事実上の民間企業への圧力、指導であり、憲法の規範を明らかに逸脱している。

「性的に搾取された子どものような社会の非常に脆弱なメンバー」の保護という理由について

暗号化に対する規制は、インターネットの草創期から繰り返し政府が要求してきたものであり、今回が初めてではない。(初期の頃の暗号をめぐる政府と暗号コミュニティとの闘いについては、シムソン・ガーフィンケル『PGP : 暗号メールと電子署名 Encryption for everyone』、ユニテック訳、オライリー・ジャパン、参照) 暗号規制は、政府の捜査機関が一般的に通信を傍受、監視する力を確保することを意図して繰り返し主張され、その都度、暗号規制はプライバシー団体やインターネットにおける市民的自由を擁護する人びとの運動によって阻まれてきた。捜査機関が暗号解読のための特権的な顕現を持ちたいという動機は、当時から現在に至るまで変るところはない。この特権を正当化するために、様々な尤もらしい理由が持ち出されているに過ぎない。通信の秘密や思想信条の自由など基本的人権は、捜査機関の権限への制約を課すことで保護されている権利であることを強調しておきたい。

一般に、「社会における脆弱な人びと」は、社会の支配的な集団から迫害、差別、搾取の対象になっている場合がほとんどである。こうした「脆弱な人びと」にとって、たとえば、支援者たちとの通信、ジャーナリストや人権団体、外部(国外)との通信など安全なコミュニケーション環境を確保する上で、暗号化は唯一の手段である。どこの国においても捜査機関がこうした「脆弱な人びと」の権利を防衛する立場に立つとは限らないことを私たちは繰り返し経験している。この点で捜査機関に暗号解読の特権を与えるような技術の導入は、むしろ「脆弱な人びと」の安全をより一層脅かすことになりかねない。

国際的な動向について
暗号規制の動きは米国を中心とする英語圏諸国と EU において活発に展開されており、これが他の諸国にも波及する傾向にある。今回のステートメントもこうした国際的な動向の一貫として理解する必要がある。暗号規制の理由は、地域によってまちまちであり、いずれの地域でも、世論の同意が得られそうな課題を前面に押し出して暗号規制を法制化し、技術として実装させようとしている点では共通している。

なお、今回のステートメントに関しては、国際的な暗号規制に反対している団体、Global Encryption Coalition からはいちはやく反対の声明が出されている。(JCA-NET も Global Encryption Coalition のメンバー団体である)
https://www.globalencryption.org/2020/10/cdt-gpd-and-internet-society-reject-time-worn-argument-for-encryption-backdoors/
(日本語訳：https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/cdt-gpd-and-internet-society-reject-time-worn-argument-for-encryption-backdoors/>)
以下時系列でここ数年の暗号化をめぐる各国政府などの主な動きをリストアップしておく。2019 年の大阪 G20 の首脳声明は、暗号化の文言はないものの事実上暗号規制に踏み出す政府間の合意を生み出すきっかけを作ったものとして重要なのでやや長く引用した。

- 2019 大阪サミット「テロ及びテロに通じる暴力的過激主義（VECT）によるインターネットの悪用の防止に関する G20 大阪首脳声明」
https://www.mofa.go.jp/mofaj/gaiko/g20/osaka19/jp/documents/final_g20_statement_on_preventing_terrorist_and_vect.html
「我々は、オンラインプラットフォームに対し、テロリストや VECT のコンテンツがインターネット中継され、アップロードされ、又は再アップロードされることを防ぐ取組の野心や速度を高めるよう、強く促す。我々は、テロリストや VECT のコンテンツを検出し、これが自らのプラットフォームに現れるのを防ぐために、サービス利用規約を設け、実施し、強制するための共同の取組を強く奨励する。その他の手段の中でも、これは技術を開発することによって達成されるかもしれない。テロリストのコンテンツがアップロード又は配信される場合、我々は、オンラインプラットフォームが、文書の証拠が保存されるよう確保しつつ、拡散を防ぐため適時にこれに対処する重要性を強調する。我々は、自らの方針や手続に設けられているとおり、定期的かつ透明性をもって公に報告するとのオンラインプラットフォームのコミットメントを歓迎する。」

- 2019 年 7 月 Five country ministerial 2019 Emerging Threats London
2019: Joint Meeting of FCM and Quintet of Attorneys-General

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822818/Joint_Meeting_of_FCM_and_Quintet_of_Attorneys_FINAL.pdf

- 20209月 Politico紙がEUj理事会の「エンド・ツー・エンド暗号化通信における子どもの性的虐待を把握する技術的解決」という内部文書を公表
https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf

- 2020年10月（米司法省国際声明)エンド・ツー・エンドの暗号化と公共の安全(本ステートメント)

- 2020年12月、欧州連合（EU）理事会は、欧州でのエンドツーエンド暗号化の使用を管理するための新しいルールの決議案

- 2020年12月、米国、財務省の金融犯罪執行ネットワーク（FinCEN）マネーサービス事業者（例えば、暗号通貨取引所を含む）に、自己ホスト型の暗号通貨ウォレットや外国の取引所を利用して顧客と取引する人々の身元データの収集を義務付ける規制案を発表
https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/eff_us_cryptcurrency_regulation/

――

資料
外務省、ホームページ
https://www.mofa.go.jp/mofaj/la_c/sa/co/page22_003432.html
エンドツーエンド暗号化及び公共の安全に関するインターナショナル・ステートメント
令和2年10月12日

10月11日、英国を始めとする関係国による暗号化に関するインターナショナル・ステートメントが発出され、我が国もこれに参加しました。同ステートメントの概要以下のとおりです（参加国：英国、米国、オーストラリア、ニュージーランド、カナダ、インド及び日本）。
ステートメント参加国は、個人情報、プライバシー、知的財産、企業秘密、サイバー・セキュリティー、報道関係者や人権擁護者の保護において中心的な役割を果たす強固な暗号化を支持。しかし、**暗号化技術は性的搾取を受けた児童のように社会の脆弱性の高い人々を含む公共の安全に対し、重大な挑戦にもなる**と指摘。

このため、参加国はテクノロジー企業に対し、政府と協力し、合理的かつ技術的に実行可能な方法に焦点を当て、以下の行動をとるよう呼びかけ。
（1）システム設計に公共の安全を取り入れることにより、企業が違法なコンテンツや活動に対し、安全性を損なうことなく効果的に行動できるようにしつつ、違法行為の捜査や訴追を円滑化し、脆弱な人々を保護することができるようにすること。
（2）**令状等が合法的に発行され、必要かつ衡平であり、厳格な手続と審査に服している場合に、法執行機関が読取可能かつ利用可能な形式のコンテンツにアクセスできるようにする**こと。
（3）合法的なアクセスを促進するための政府や他の利害関係者との協議に、実質的かつ設計の決定に実際に影響を及ぼす形で取り組むこと。参加国は、テクノロジー企業と政府が公衆とそのプライバシーを保護し、サイバー・セキュリティーと人権を擁護し、技術革新を支援することを可能にする合理的な方策を立案するため、企業と共に取り組むことを約束することを表明。

2021年9月G7 内務大臣コミットメント(抜粋)
「我々は、テロリズムや児童虐待などの重大な**犯罪の捜査・訴追に不可欠な通信コンテンツへの合法的なアクセス(*)**を厳格に管理するために協力する
我々は、市民の安全を守るために、インターネット技術企業と協力してこれを行う。
我々は、インターネット技術企業に対して、この責任を認識し、行動することを求める。」

(*)コンテンツとは、通信が暗号化されていて解読できない場合、復号化して読むことができるようにされた内容のことを示唆している。「合法的なアクセス」は、暗号コンテンツを復号化して読むことを法制度として認めるべきであるということを示唆し、民間企業の協力もまた法的に義務づけることを示唆している。

JCA-NET の目的

JCA-NET は通信 NGO として、APC（進歩的コミュニケーション協会）とともに、世界の APC メンバー 40 カ国以上のパートナーとの協力により、社会的、環境的、経済的正義、性による差別の克服を求める社会運動を、情報通信技術を使って支援します。

新しいインターネット時代に

いま、情報通信の環境は変化しています。そして、情報通信の環境の変化が社会の構造の変化を促す時代がやってこようとしています。その環境は時として暴力的で、集権的で、差別的でもあります。時代に対抗するため、JCA-NET は情報通信技術の民衆的コントロールを通じてインターネット社会の民主化に貢献し、インターネットコミュニティの形成に参画します。
JCA-NET はインターネット、コンピュータを市民運動の道具として活用していくことを支援する組織がほしい、という NGO、NPO、市民運動団体の人たち、コンピュータ技術者の人たちの声によって生み出されました。
JCA-NET はインターネットプロバイダでもあります。ユーザーと会員が使いやすい道具を提供することによって、市民社会の強固な基盤づくりのために活動します。

JCA-NET でできること

1．JCA-NET は市民団体・グループの情報ツールを提供します
＊Web パブリッシングサーバ、会議室／Web 連動メーリングリスト ＊独自ドメインも安価で使えます。
市民運動の声を効果的に発信しよう！
市民運動団体の活動の中で生まれてきた情報を効果的に、グループ内で、あるいは広報用に効果的に使うことができるシステム。JCA-NET は市民運動に特化していますから、市民運動に関する情報の密度が高い。JCA-NET Search! では中身の濃い全文情報検索が可能です！
市民運動の活動記録をしっかり蓄積しよう！
JCA-NET では市民運動の活動記録を残していくためにも、市民運動に関する情報記録に関しては容量制限をかけません。団体名のディレクトリ、独自ドメイン、サブドメインも使えます。
2．JCA-NET 広報システム
JCA-NET では効果的に社会に情報発信をするためのメール／Web マガジンを構築しています。 このシステムの活用によって、自分たちの活動を効果的に広げることができます。
3．サポート、コンピュータ市民講座への取り組み
JCA-NET では市民運動がコンピュータやインターネットなどの ICT（情報コミュニケーション技術）を効果的に使えるように、出張サポートやコンピュータ・インターネットに関する出張講座などをやっています。自分たちの団体のメンバー対象に要望に沿ったカリキュラムを作ることも可能です。
プライバシーを守る運用ポリシーとユーザサイドのスキルアップを！
JCA-NET では、他のプロバイダには見られないプライバシー保護の取り組みをしています。また、ネットワーク時代のプライバシーを守るための技術講座も定期的に開催しています。

問い合わせ：office@jca.apc.org

https://www.jca.apc.org/jca-net/ja